

PATENT
81784.0289
Express Mail Label No. EV 324 110 896 US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	Art Unit: Not assigned
Yutaka KANEKO	Examiner: Not assigned
Serial No: Not assigned	
Filed: November 3, 2003	
For: Optical Disk Drive, Optical Disk, Security Control Method for Optical Disk Drive, and Security Control Program for Optical Disk Drive	

TRANSMITTAL OF PRIORITY DOCUMENT

Mail Stop PATENT APPLICATION
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

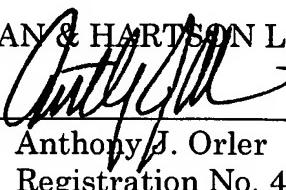
Enclosed herewith is a certified copy of Japanese patent application No. 2002-360851 which was filed December 12, 2002, from which priority is claimed under 35 U.S.C. § 119 and Rule 55.

Acknowledgment of the priority document(s) is respectfully requested to ensure that the subject information appears on the printed patent.

Respectfully submitted,

HOGAN & HARTSON L.L.P.

Date: November 3, 2003

By: 

Anthony J. Orler
Registration No. 41,232
Attorney for Applicant(s)

500 South Grand Avenue, Suite 1900
Los Angeles, California 90071
Telephone: 213-337-6700
Facsimile: 213-337-6701

Translation of Priority Certificate

JAPAN PATENT OFFICE

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application: December 12, 2002

Application Number: Patent Application

No. 2002-360851

[ST.10/C]: [JP2002-360851]

Applicant(s): SANYO ELECTRIC CO., LTD.

July 2, 2003

**Commissioner, Japan Patent Office
Shinichiro Ota**

Priority Certificate No. 2003-3052420

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日

Date of Application: 2002年12月12日

出願番号

Application Number: 特願2002-360851

[ST.10/C]:

[JP2002-360851]

出願人

Applicant(s): 三洋電機株式会社

2003年 7月 2日

特許庁長官
Commissioner,
Japan Patent Office

太田信一郎

出証番号 出証特2003-3052420

【書類名】 特許願
 【整理番号】 JAB1020113
 【提出日】 平成14年12月12日
 【あて先】 特許庁長官殿
 【国際特許分類】 G06F 7/00
 G06F 11/00

【発明者】

【住所又は居所】 大阪府守口市京阪本通2丁目5番5号 三洋電機株式会社内

【氏名】 金子 豊

【特許出願人】

【識別番号】 000001889

【氏名又は名称】 三洋電機株式会社

【代理人】

【識別番号】 100075258

【弁理士】

【氏名又は名称】 吉田 研二

【電話番号】 0422-21-2340

【選任した代理人】

【識別番号】 100096976

【弁理士】

【氏名又は名称】 石田 純

【電話番号】 0422-21-2340

【手数料の表示】

【予納台帳番号】 001753

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1
【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 光ディスク装置、光ディスク、光ディスク装置のセキュリティ管理方法及び光ディスク装置のセキュリティ管理プログラム

【特許請求の範囲】

【請求項1】 データとデータに対するセキュリティ情報を光ディスクに記録する手段であって、同一のセキュリティ情報を光ディスクの複数箇所に記録する記録手段と、

光ディスクからデータ及びセキュリティ情報を読み出す読取手段と、

データを読み出す際に、読み出す対象となるデータに対するセキュリティ情報に基づいてデータの読み出しを制限する手段であって、複数箇所から読み出されたセキュリティ情報を対比することによって、最も出現頻度の高いセキュリティ情報に基づいて前記読み出す対象となるデータの読み出しを制限するアクセス制限手段と、

を備えることを特徴とする光ディスク装置。

【請求項2】 データ及びデータに対する同一のセキュリティ情報が複数箇所に記録された光ディスクからデータを読み出す光ディスク装置であって、

前記光ディスクからデータ及びセキュリティ情報を読み出す読取手段と、

データに読み出す際に、読み出す対象となるデータに対するセキュリティ情報に基づいてデータの読み出しを制限する手段であって、複数箇所から読み出されたセキュリティ情報を対比することによって、最も出現頻度の高いセキュリティ情報に基づいて前記読み出す対象となるデータの読み出しを制限するアクセス制限手段と、

を備えることを特徴とする光ディスク装置。

【請求項3】 請求項1又は2に記載の光ディスク装置において、

前記セキュリティ情報は、連続するビット列で表される情報であり、

前記アクセス制御手段は、前記複数箇所からセキュリティ情報として読み出されたビット値をビット列毎に比較し、ビット列毎に最も出現頻度が高いビット値を当該ビット列の正しいビット値とすることを特徴とする光ディスク装置。

【請求項4】 請求項1～3のいずれか1つに記載の光ディスク装置におい

て、

前記読み取手段によって読み出されたデータの誤り頻度を検出するエラー検出手段を更に含み、

前記アクセス制限手段は、前記エラー検出手段によって得られたデータの誤り頻度に基づいてセキュリティ情報を補正することを特徴とする光ディスク装置。

【請求項5】 記録対象となるデータと、当該データに対するセキュリティ情報を光ディスクに記録する手段であって、同一のセキュリティ情報を光ディスクの複数箇所に記録する記録手段を備えることを特徴とする光ディスク装置。

【請求項6】 記録対象となるデータと、当該データに対するセキュリティ情報とが記録された光ディスクであって、同一のセキュリティ情報が複数箇所に記録されていることを特徴とする光ディスク。

【請求項7】 データ及びデータに対する同一のセキュリティ情報が複数箇所に記録された光ディスクのデータを管理する光ディスク装置のセキュリティ管理方法であって、

管理対象となるデータに対するセキュリティ情報を光ディスクの複数箇所から読み出すセキュリティ情報読み取工程と、

前記複数箇所から読み出されたセキュリティ情報を対比することによって、最も出現頻度の高いセキュリティ情報を正当セキュリティ情報として決定するセキュリティ情報決定工程と、

を含み、

前記正当セキュリティ情報を前記管理対象となるデータの処理に供することを特徴とする光ディスク装置のセキュリティ管理方法。

【請求項8】 請求項7に記載の光ディスク装置のセキュリティ管理方法において、

前記セキュリティ情報は、連続するビット列で表される情報であり、

前記セキュリティ情報決定工程は、前記複数箇所から読み出されたビット値をビット列毎に比較し、ビット列毎に最も出現頻度が高いビット値を当該ビット列のビット値とすることを特徴とする光ディスク装置のセキュリティ管理方法。

【請求項9】 請求項7又は8に記載の光ディスク装置のセキュリティ管理

方法において、

前記光ディスクに記録されたデータの誤り頻度を検出するエラー検出工程をさらに含み、

前記セキュリティ情報決定工程は、前記誤り頻度に基づいて正しいセキュリティ情報を決定することを特徴とする光ディスク装置のセキュリティ管理方法。

【請求項10】 データ及びデータに対する同一のセキュリティ情報が複数箇所に記録された光ディスクのデータを管理する光ディスク装置のセキュリティ管理プログラムであって、

コンピュータに、

管理対象となるデータに対するセキュリティ情報を光ディスクの複数箇所から読み出すセキュリティ情報読取工程と、

前記複数箇所から読み出されたセキュリティ情報を対比することによって、最も出現頻度の高いセキュリティ情報を正当セキュリティ情報として決定するセキュリティ情報決定工程と、

を含む処理を実行させることを特徴とする光ディスク装置のセキュリティ管理プログラム。

【請求項11】 請求項10に記載の光ディスク装置のセキュリティ管理プログラムにおいて、

前記セキュリティ情報は、連続するビット列で表される情報であり、

前記セキュリティ情報決定工程は、前記複数箇所から読み出されたビット値をビット列毎に比較し、ビット列毎に最も出現頻度が高いビット値を当該ビット列のビット値とすることを特徴とする光ディスク装置のセキュリティ管理プログラム。

【請求項12】 請求項11又は12に記載の光ディスク装置のセキュリティ管理プログラムにおいて、

コンピュータに、前記光ディスクに記録されたデータの誤り頻度を検出するエラー検出工程をさらに実行させ、

前記セキュリティ情報決定工程において、前記誤り頻度に基づいて正しいセキュリティ情報を決定することを特徴とする光ディスク装置のセキュリティ管理プ

ログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、コンパクトディスク及びデジタル多目的ディスク等の光ディスクシステムにおいてセキュリティ性及びアクセス性を向上した光ディスク装置、光ディスク、光ディスク装置のセキュリティ管理方法及び光ディスク装置のセキュリティ管理プログラム方法に関する。

【0002】

【従来の技術】

動画記録等の大容量データ記録の必要性が高まり、高密度記録型コンパクトディスク（HD-Burn-CD：High-Density-Burn-type）及びデジタル多目的ディスク（DVD）が広く使用されている。

【0003】

このような大容量の記憶装置においては、そこに記憶されたデータの改竄や、アクセス権を持たない者からの不正なデータの読み出しを防ぐことがセキュリティ上の課題となっている。

【0004】

特開平2001-35092号公報には、光ディスク等のリムーバブルメモリのセキュリティを向上する技術が開示されている。当該技術では、リムーバブルメモリのメモリ空間において一般ユーザが書き換え不能な管理領域を予め定めておき、その管理領域にユーザのパスワード等のセキュリティ情報を埋め込み、リムーバブルメモリにアクセスする際にはユーザから確認用の情報の入力を行わせ、管理領域に埋め込まれたセキュリティ情報とユーザが入力した確認用の情報とを対比して所定の条件を満たせばリムーバブルメモリへのアクセスを可能にする。

【0005】

【特許文献1】

特開平2001-35092号公報

【0006】

【発明が解決しようとする課題】

しかしながら、上記従来技術では、リムーバブルディスク上に一般ユーザが容易にアクセスできない管理領域を設けておく必要があった。管理領域にはリムーバブルディスク上に記録される全データに対する管理データが記録されるため、管理領域として予め広い記憶領域を割り当てておく必要があり、実際に利用できる記録領域が減少する等の問題があった。

【0007】

また、上記従来技術では、リムーバブルディスク上の全データに対するセキュリティ情報が管理領域に集中して記録される。そのため、セキュリティ情報を盗み見ようとする者がセキュリティ情報を発見し易くなり、セキュリティ情報の漏洩や改竄等の問題が起こりやすい状況にあった。

【0008】

さらに、データを記録又は読み取る際に、ディスク装置のヘッドをリムーバブルディスク上のデータ記録領域と管理領域との間で頻繁に移動させる必要がある。そのため、データへのアクセス時間が長くなる問題があった。

【0009】

本発明は、上記従来技術の問題を鑑み、少なくとも上記課題の一つを解決するべく、改良されたセキュリティ管理を可能とする光ディスク装置、光ディスク、光ディスク、光ディスク装置のセキュリティ管理方法及び光ディスク装置のセキュリティ管理プログラムを提供することを目的とする。

【0010】

【課題を解決するための手段】

上記課題を解決できる本発明は、データとデータに対するセキュリティ情報を光ディスクに記録する手段であって、同一のセキュリティ情報を光ディスクの複数箇所に記録する記録手段と、光ディスクからデータ及びセキュリティ情報を読み出す読み取り手段と、データを読み出す際に、読み出す対象となるデータに対するセキュリティ情報に基づいてデータの読み出しを制限する手段であって、複数箇所から読み出されたセキュリティ情報を対比することによって、最も出現頻度の

高いセキュリティ情報に基づいて前記読み出す対象となるデータの読み出しを制限するアクセス制限手段とを備えることを特徴とする光ディスク装置である。

【0011】

ここで、本発明は、データ及びデータに対する同一のセキュリティ情報が複数箇所に記録された光ディスクからデータを読み出す光ディスク装置であって、前記光ディスクからデータ及びセキュリティ情報を読み出す讀取手段と、データに読み出す際に、読み出す対象となるデータに対するセキュリティ情報に基づいてデータの読み出しを制限する手段であって、複数箇所から読み出されたセキュリティ情報を対比することによって、最も出現頻度の高いセキュリティ情報に基づいて前記読み出す対象となるデータの読み出しを制限するアクセス制限手段とを備えることを特徴とする。

【0012】

より具体的には、前記セキュリティ情報は、連続するビット列で表される情報であり、前記アクセス制御手段は、前記複数箇所からセキュリティ情報として読み出されたビット値をビット列毎に比較し、ビット列毎に最も出現頻度が高いビット値を当該ビット列の正しいビット値とすることを特徴とすることが好適である。

【0013】

さらに、上記光ディスク装置において、前記讀取手段によって読み出されたデータの誤り頻度を検出するエラー検出手段を更に含み、前記アクセス制限手段は、前記エラー検出手段によって得られたデータの誤り頻度に基づいてセキュリティ情報を補正することが好ましい。

【0014】

上記課題を解決できる本発明の別の態様は、記録対象となるデータと、当該データに対するセキュリティ情報を光ディスクに記録する手段であって、同一のセキュリティ情報を光ディスクの複数箇所に記録する記録手段を備えることを特徴とする光ディスク装置である。

【0015】

上記課題を解決できる本発明の別の態様は、記録対象となるデータと、当該デ

ータに対するセキュリティ情報とが記録された光ディスクであって、同一のセキュリティ情報が複数箇所に記録されていることを特徴とする光ディスクである。

【0016】

上記課題を解決できる本発明の別の態様は、データ及びデータに対する同一のセキュリティ情報が複数箇所に記録された光ディスクのデータを管理する光ディスク装置のセキュリティ管理方法であって、管理対象となるデータに対するセキュリティ情報を光ディスクの複数箇所から読み出すセキュリティ情報読取工程と、前記複数箇所から読み出されたセキュリティ情報を対比することによって、最も出現頻度の高いセキュリティ情報を正当セキュリティ情報として決定するセキュリティ情報決定工程とを含み、前記正当セキュリティ情報を前記管理対象となるデータの処理に供することを特徴とする。

【0017】

より具体的には、前記セキュリティ情報は、連続するビット列で表される情報であり、前記セキュリティ情報決定工程は、前記複数箇所から読み出されたビット値をビット列毎に比較し、ビット列毎に最も出現頻度が高いビット値を当該ビット列のビット値とすることが好適である。

【0018】

さらに、上記光ディスク装置のセキュリティ管理方法において、前記光ディスクに記録されたデータの誤り頻度を検出するエラー検出工程をさらに含み、前記セキュリティ情報決定工程は、前記誤り頻度に基づいて正しいセキュリティ情報を決定することが好ましい。

【0019】

上記課題を解決できる本発明は、データ及びデータに対する同一のセキュリティ情報が複数箇所に記録された光ディスクのデータを管理する光ディスク装置のセキュリティ管理プログラムであって、コンピュータに、管理対象となるデータに対するセキュリティ情報を光ディスクの複数箇所から読み出すセキュリティ情報読取工程と、前記複数箇所から読み出されたセキュリティ情報を対比することによって、最も出現頻度の高いセキュリティ情報を正当セキュリティ情報として決定するセキュリティ情報決定工程とを含む処理を実行させることを特徴とする

【0020】

より具体的には、前記セキュリティ情報は、連続するビット列で表される情報であり、前記セキュリティ情報決定工程は、前記複数箇所から読み出されたビット値をビット列毎に比較し、ビット列毎に最も出現頻度が高いビット値を当該ビット列のビット値とすることが好適である。

【0021】

さらに、上記光ディスク装置のセキュリティ管理プログラムにおいて、コンピュータに、前記光ディスクに記録されたデータの誤り頻度を検出するエラー検出工程をさらに実行させ、前記セキュリティ情報決定工程において、前記誤り頻度に基づいて正しいセキュリティ情報を決定することが好ましい。

【0022】

【発明の実施の形態】

本発明の実施の形態について、図を参照して詳細に説明する。

【0023】

<装置構成>

本発明の実施の形態における光ディスク装置100の構成は、図1のように、制御部10、記憶部12、データエンコーダ14、光学系制御部16、光学ヘッド18、ATIPデコーダ20、データデコーダ22、モータ制御部24、モータ26及びインターフェース28から基本的に構成される。

【0024】

光ディスク装置100は、インターフェース28を介して外部装置と情報伝達可能に接続され、例えば外部に置かれたホストコンピュータ等に対してデータの入出力を行うことができる。

【0025】

制御部10は、記憶部12、データエンコーダ14、光学系制御部16、データデコーダ22及びインターフェース28と情報伝達可能に接続され、記憶部12に格納された制御プログラムを実行することによって光ディスク装置100の制御を統括する。制御部10は、インターフェース28から受け取ったデータを

記憶部12に一旦格納し、隨時読み出してデータエンコーダ14に送出する。

【0026】

データエンコーダ14は、制御部10からの制御命令に従って、受信したデータを光ディスクに記録するためのデータフォーマットに変換し、光学系制御部16に出力する。

【0027】

光学系制御部16は、制御部10からのデータ書き込み命令を受け、光学ヘッド18を制御することによってデータエンコーダ14から受けたデータを光ディスクに書き込む。また、制御部10からのデータ読み込み命令を受け、光学ヘッド18を制御することによって光ディスクから読み出したデータをデータデコーダ22及びATIPデコーダ20に出力する。

【0028】

光学ヘッド18は、レーザ、レンズ、駆動装置等を含み、光ディスク上にデータを書き込み、又は光ディスクからデータを読み取る。例えば、DVDでは650nmの波長のレーザを用いることができる。

【0029】

ATIPデコーダ20は、光ディスクから抽出されるウォブル信号からATIP(Absolute Time In Pre-groove)アドレスを復調し、モータ制御部24に出力する。

【0030】

データデコーダ22は、光ディスクから読み出されたデータを受けて、受信したデータの復調を行い、制御部10へ送出する。

【0031】

モータ制御部24は、ATIPデコーダ20からATIPアドレスを受けて、スピンドルモータ26を制御することによって光ディスクの回転を調整する。例えば、ATIPアドレスと同期をとって光ディスクを線速度一定に回転制御する。

【0032】

〈データ及びセキュリティ情報の記録処理〉

以下、図を参照して、本実施の形態におけるデータ及びセキュリティ情報の記録処理について詳細に説明する。本実施の形態における記録処理は、図2のフローチャートに示す各工程をプログラム化して記憶部12に記憶させておき、制御部10で実行することによって行うことができる。

【0033】

ステップS10では、記録対象となるデータを外部装置から受信し、受信したデータをデータブロックに分割する。データブロックとしては、例えば、リード・ソロモン積符号方式におけるECC（積符号）データブロックを用いることができる。このリード・ソロモン積符号方式では、32kBの実データに対して5kBの誤り訂正用の冗長データ（パリティ）が付加された合計37kBのECC（積符号）データブロックによって誤り訂正が行われる。

【0034】

図3に示すように、データを1バイト単位のデータD0, D1…Dn毎に、所定のデータ単位k毎に縦方向に折り返しながら読み出した順に横方向に行列配置する。さらに、図4に示すように、データDi,j（i, jは行列番号）がブロック化されると、各々の行及び列毎に冗長データPI, POを付与する。横方向の各行を内符号と呼び、縦方向の各列を外符号と呼ぶ。通常、内符号系列RはRS(182, 172, 11)、外符号系列CはRS(208, 192, 17)と記載される。ここで、RS(n, k, d)において、nは符号長、kは情報記号長、dは符号語間の最小距離を示す。

【0035】

このリード・ソロモン積符号方式は強力な誤り訂正機能を有しており、ECCデータブロック内に生ずる僅かな誤りを完全に修正することができる。本発明では、この強力な誤り訂正機能を利用する。

【0036】

ステップS12では、外部装置からセキュリティ情報を受信し、受信したセキュリティ情報を複数のECCデータブロックに埋め込む。セキュリティ情報を埋め込むECCデータブロックの数は記録処理前に予め定めておくことができる。

【0037】

例えば、記録対象となるデータに対するセキュリティ情報が3バイトの情報量であり、その値が55h, 76h, 98hであったとする。1つのセキュリティ情報を5つのECCデータブロックに埋め込むことと予め設定されている場合、図5に示すように、記録対象となるデータから得られた5つのECCデータブロックにおいて最初のデータ値から順にセキュリティ情報に置き換える。

【0038】

このとき、セキュリティ情報を埋め込むECCデータブロックはランダムに選択しても良い。また、セキュリティ情報を埋め込む位置は予め定められていれば、ECCデータブロックにおけるデータ領域のいずれの場所に埋め込んでも良い。

【0039】

さらに、セキュリティ情報が複数ある場合には、それらのセキュリティ情報を1つのECCデータブロックに埋め込んでも良い。ただし、1つのECCデータブロックに埋め込むセキュリティ情報数は、記録及び読取を通じて発生する誤りをリード・ソロモン積符号方式で訂正できる程度に抑えることが好ましい。従って、セキュリティ情報の情報量が誤り訂正できない程度に大きい場合には、セキュリティ情報を分割してECCデータブロックに振り分けて埋め込むことが好適である。

【0040】

例えば、内符号系列RS(182, 172, 11)及び外符号系列RS(208, 192, 17)のリード・ソロモン積符号方式を用いた場合、バースト誤りが生じないものとすると、誤り訂正可能なデータの個数は93バイトとなる。

【0041】

ステップS14では、セキュリティ情報が埋め込まれたECCデータブロックの情報を実際に光ディスクに記録する。例えば、セキュリティ情報が埋め込まれたことをディスクの管理情報に記録しておくことが好適である。

【0042】

以上の処理によって、光ディスク上にデータ及びセキュリティ情報に記録することができる。

【0043】**<データ及びセキュリティ情報の読み取り処理>**

以下、図を参照して、本実施の形態におけるデータ及びセキュリティ情報の読み取り処理について詳細に説明する。本実施の形態における記録処理は、図6のフローチャートに示す各工程をプログラム化して記憶部12に記憶させておき、制御部10で実行することによって行うことができる。

【0044】

ステップS20では、外部装置からの指令を受けて、光ディスク装置の管理情報等を読み出し、読み出し対象となるデータにセキュリティ情報が記録されているか否かを確認する。セキュリティ情報が埋め込まれていればステップS22に処理を移行し、セキュリティ情報が埋め込まれていなければステップS30に処理を移行する。

【0045】

ステップS22では、読み出し対象となるデータに埋め込まれているセキュリティ情報を抽出して外部装置に送出する。

【0046】

まず、光ディスク上のデータ領域にアクセスし、読み出し対象となるデータをECCデータブロックに再構築する。次に、リード・ソロモン積符号方式に基づいて、ECCデータブロックのデータの誤り訂正を行う。このとき、ECCデータブロック間においてデータの誤り率の比較を行い、誤り率が高いECCデータブロックにセキュリティ情報が埋め込まれているものと判断し、セキュリティ情報が埋め込まれていると判断されたECCデータブロックの所定位置からセキュリティ情報を抽出する。

【0047】

例えば、図5の例のようにECCデータブロックの最初の3バイトにセキュリティ情報が埋め込まれたデータを読み出し、図7に示すようにECCデータブロックが再現されたものとする。ここで、黒塗りのデータはデータの記録処理又はデータの読み取り処理の際に誤りが生じたデータを示す。

【0048】

各ECCデータブロックには、一般的にほぼ同じ確率でデータの誤りが生ずる。セキュリティ情報自体がデータの誤りであるものと認識されるため、セキュリティ情報が埋め込まれたECCデータブロックのデータの誤り率は、セキュリティ情報が埋め込まれていないECCデータブロックの誤り率よりも高くなる。図7の例では、ECCデータブロック1～5にセキュリティ情報が埋め込まれているため、他のECCデータブロックよりも誤り率が高くなっている。これらのECCデータブロックからセキュリティ情報を抽出すれば良いことが判断できる。

【0049】

このとき、なんらかの偶発的事情により、ECCデータブロック8のように誤り率が高くなった場合、本来セキュリティ情報が埋め込まれていないECCデータブロックからもセキュリティ情報が抽出されることとなる。この場合の処理については後に詳細に説明する。

【0050】

ステップS24では、複数のECCデータブロックから抽出されたセキュリティ情報を比較し、セキュリティ情報の誤りを修正する。

【0051】

例えば、図7の例から読み出されたセキュリティ情報の最上位のデータが、55h, 75h, 55h, 4Dh及び55hとして抽出されたものとする。また、セキュリティ情報が埋め込まれていなかったECCデータブロックからも97hという情報が誤って抽出されたものとする。

【0052】

そこで、図8に示すように、抽出されたセキュリティ情報を同一ビット列毎に比較し、高い頻度で現れるビット値をそのビット列における正しいビット値として採用する。例えば、最上位ビットは0, 0, 0, 0, 0, 1であり、「0」が5つ及び「1」が1つ出現するので、最上位ビットの正しいビット値は「0」とする。

【0053】

また、セキュリティ情報の抽出元となったECCデータブロックのデータ誤り率によって各ビット列に重み付けをして処理を行うことも好適である。すなわち

、抽出元となったECCデータブロックのデータ誤り率が高い場合には、そこから抽出されたセキュリティ情報が誤っている可能性も高くなると考えられるため、データ誤り率の高いECCデータブロックから抽出されたセキュリティ情報の重要性が低く見積もられるように重み付けする。

【0054】

このように、複数抽出されたセキュリティ情報を比較し、最も出現頻度が高いセキュリティ情報を正当なセキュリティ情報として採用することによって、データに埋め込んだセキュリティ情報に誤りが発生したり、セキュリティ情報が埋め込まれていないECCデータブロックから誤ってセキュリティ情報が抽出されたりした場合にも、正しいセキュリティ情報を得られる可能性を高めることができる。

【0055】

ステップS26では、データの読み出しを制限するか否かを判断するために、ユーザ等から確認情報を取得する。この確認情報は、外部装置から取得される。

【0056】

ステップS28では、ステップS24で抽出された正当なセキュリティ情報と、ステップS26で取得された確認情報が比較される。抽出された正当なセキュリティ情報と確認情報が一致していればステップS30に処理を移行し、一致していないければステップS32に処理を移行する。

【0057】

このとき、セキュリティ情報に誤りが多く発生していたり、バースト誤り等の影響によりセキュリティ情報が多く誤って読み出されたりした場合に、ステップS24においてセキュリティ情報を完全に修正できなくなることも考慮して、抽出された正当なセキュリティ情報と確認情報とが完全に一致していなくとも、ある程度一致していれば良いものとすることもできる。

【0058】

ステップS30では、アクセスが許可できるものとして、読み出し対象となるデータを光ディスクから読み出して外部装置に送信する。外部装置は、ユーザにデータを提示する。一方、ステップS32では、データの読み出しを拒否する。

例えば、光ディスクを強制的に装置から排出させる処理等を行っても良い。

【0059】

なお、本実施の形態では、リード・ソロモン積符号化方式に基づいてデータの誤り訂正を行うものとして説明を行ったが、これに限られるものではなく、他の誤り訂正方式を用いた場合でも同様に処理することができる。

【0060】

以上のように、本実施の形態によれば、光ディスクに記録されたデータにユーザー名、パスワード、暗号鍵等のセキュリティ情報を埋め込むことによって、セキュリティ性を高めたデータの保存が可能となる。

【0061】

その結果、例えば、セキュリティ情報がデータに埋め込まれて記録されるため、光ディスク上に設ける管理領域が小さくすることができる。さらに、光ディスク上でセキュリティ情報が分散して記録されるため、セキュリティ情報の漏洩や改竄を行い難くなり、アクセス時間を短縮できる。

【0062】

【発明の効果】

本発明によれば、コンパクトディスク及びデジタル多目的ディスク等の光ディスクシステムにおいてセキュリティ性及びアクセス性を向上した光ディスク装置、光ディスク、光ディスク装置のセキュリティ管理方法及び光ディスク装置のセキュリティ管理プログラム方法を実現することができる。

【図面の簡単な説明】

【図1】 本発明の実施の形態における光ディスク装置の構成を示すブロック図である。

【図2】 本発明の実施の形態におけるデータ記録処理のフローチャートを示す図である。

【図3】 データ列からのデータブロックの構成を説明する図である。

【図4】 リード・ソロモン積符号方式の積符号データブロックの例を示す図である。

【図5】 本実施の形態におけるデータブロックへのセキュリティ情報の埋

め込み処理を説明する図である。

【図6】 本発明の実施の形態におけるデータ読み出し処理のフローチャートを示す図である。

【図7】 本発明の実施の形態におけるデータブロックからのセキュリティ情報の読み出し処理を説明する図である。

【図8】 本発明の実施の形態におけるセキュリティ情報の比較・修正処理を説明する図である。

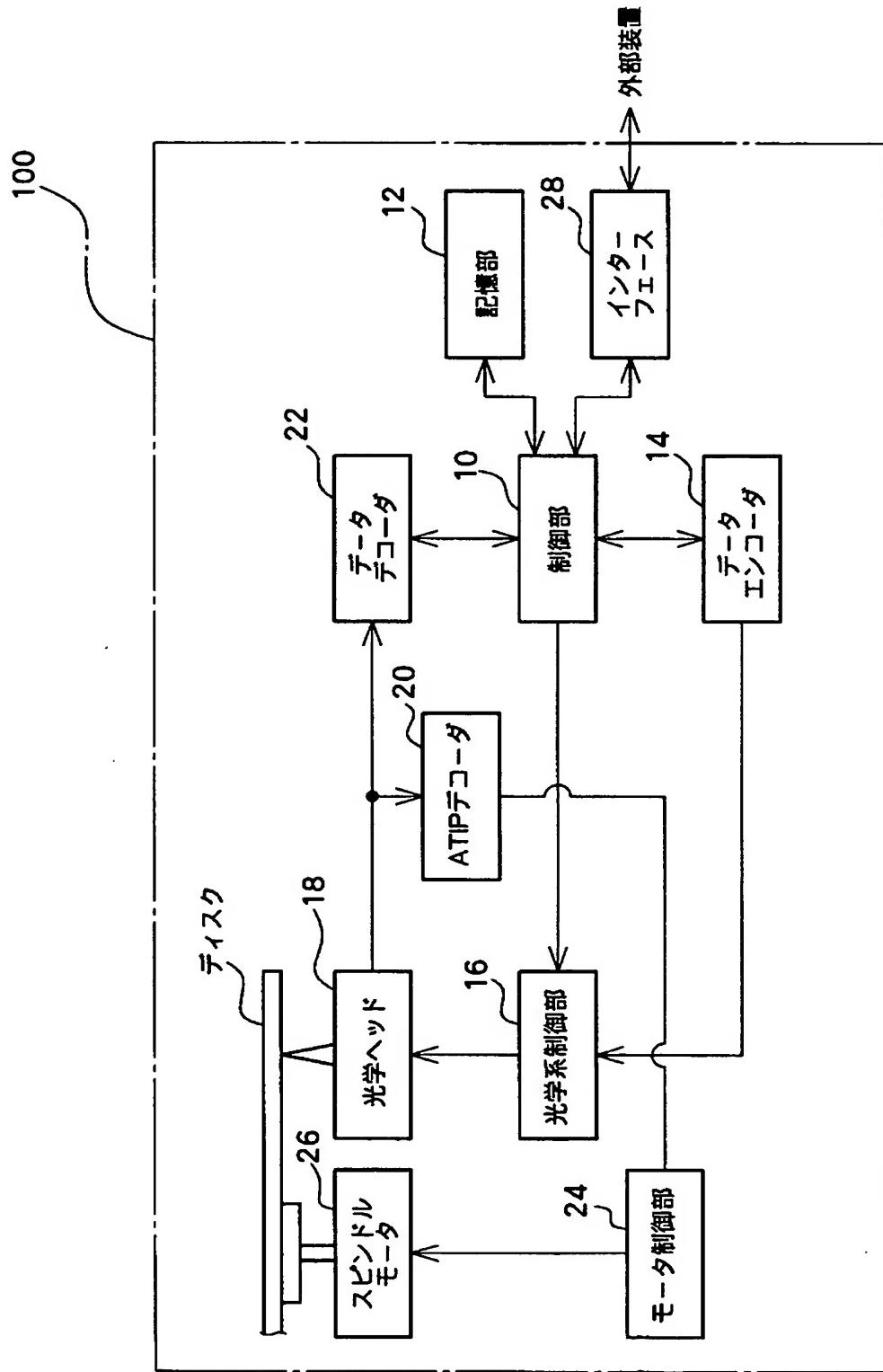
【符号の説明】

10 制御部、12 記憶部、14 データエンコーダ、16 光学系制御部、
18 光学ヘッド、20 デコーダ、22 データデコーダ、24 モータ制御部、
26 スピンドルモータ、28 インターフェース、100 光ディスク装置。

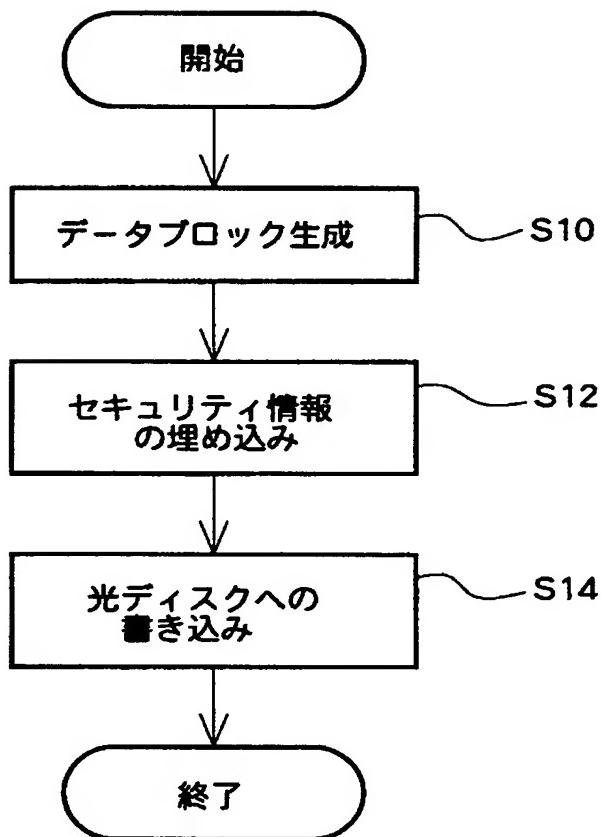
【書類名】

図面

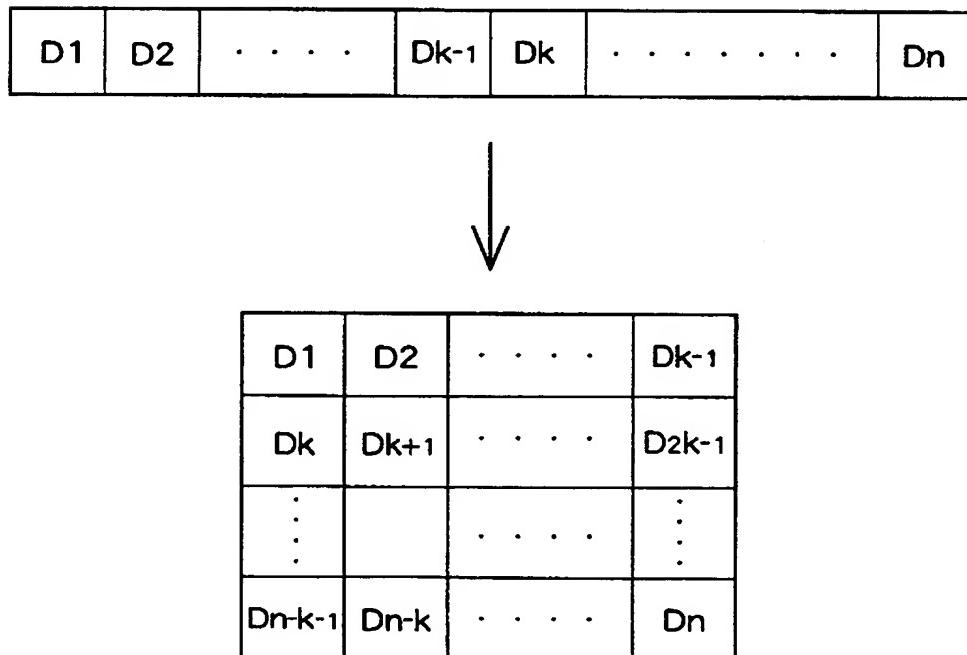
【図1】



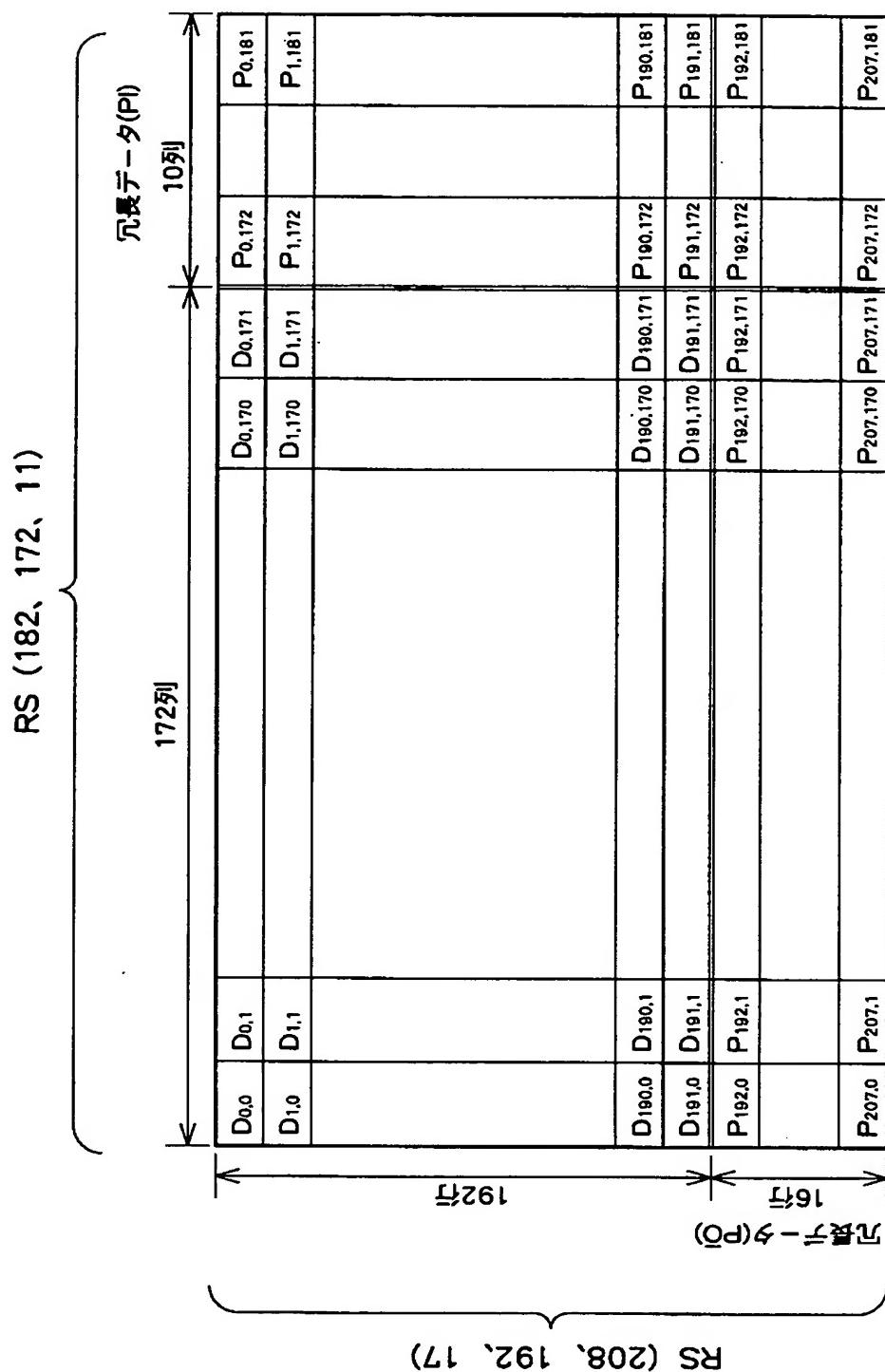
【図2】



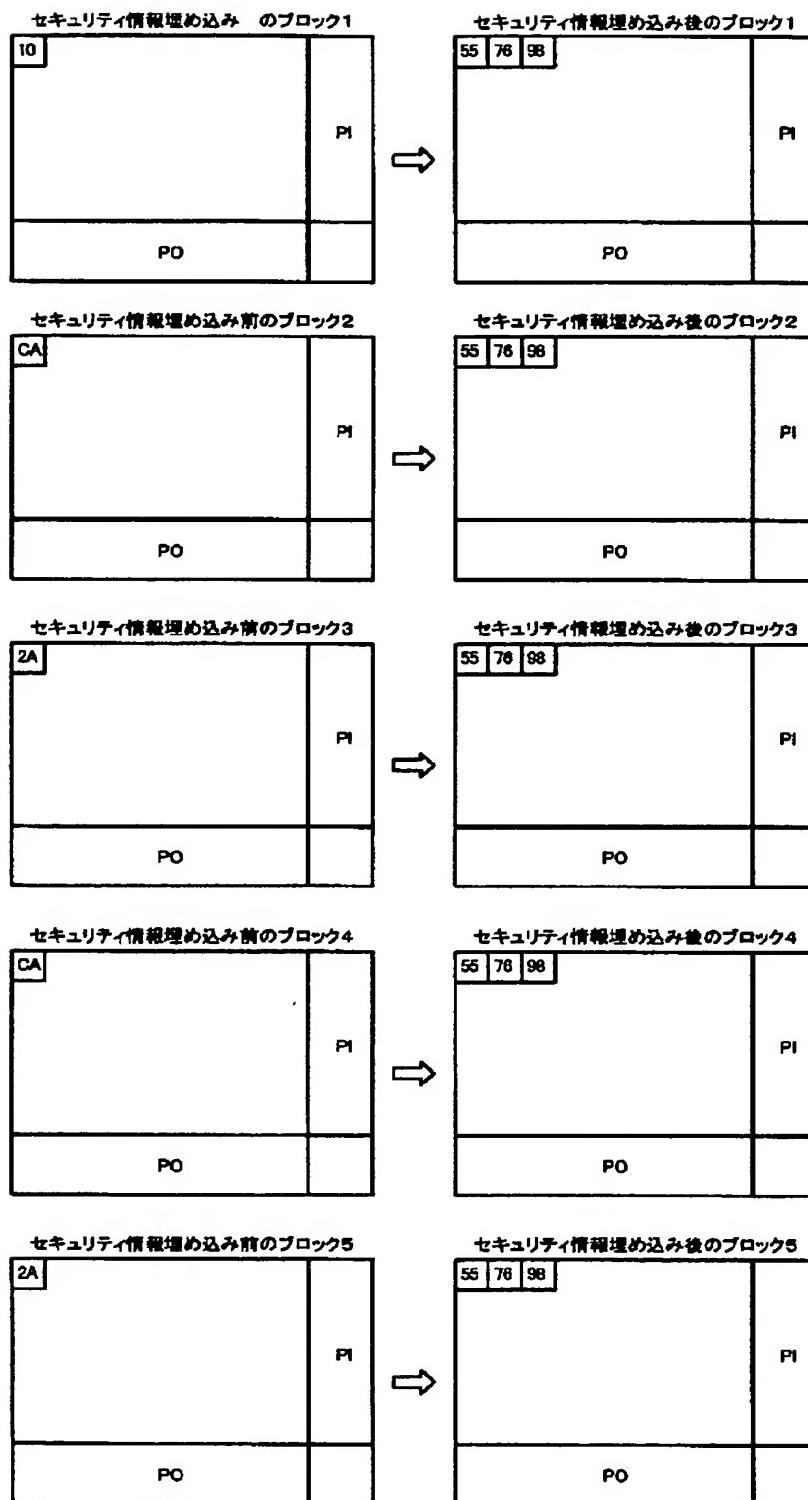
【図3】



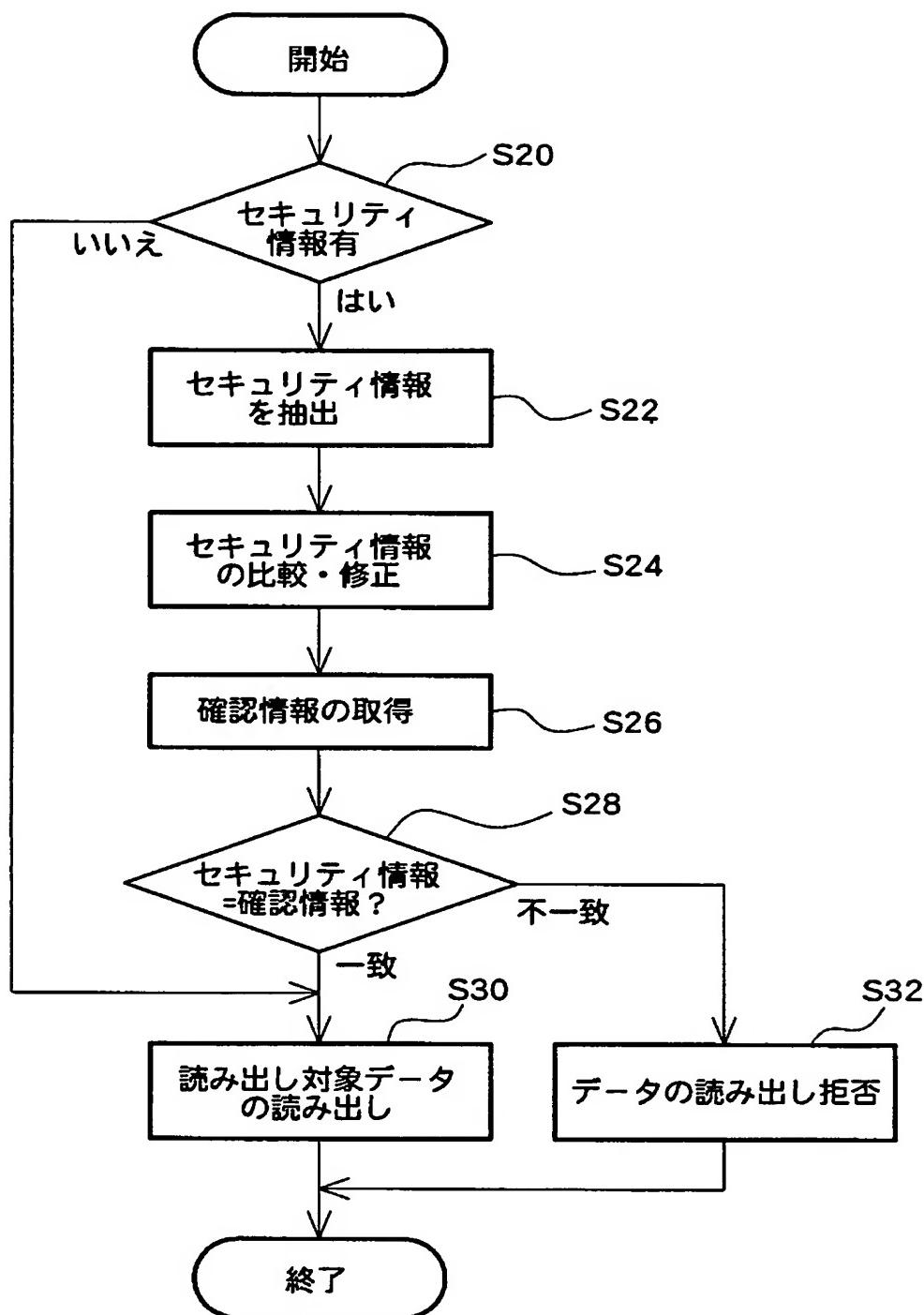
【図4】



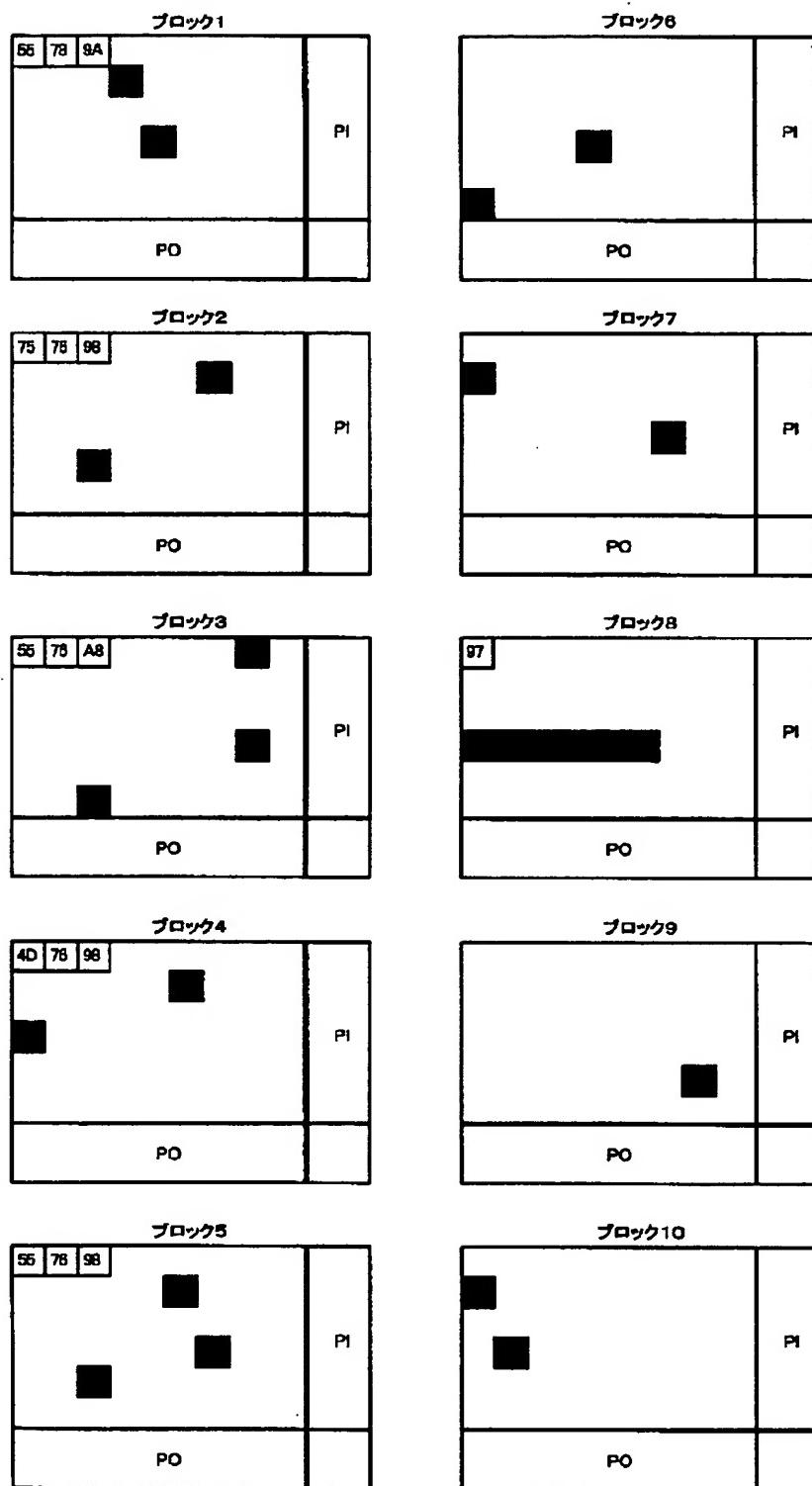
【図5】



【図6】



【図7】



【図8】

	セキュリティ情報	セキュリティ情報				ビット列
		上位4ビット		下位4ビット		
ECCデータブロック1	55h	0	1	0	1	0 1 0 1
ECCデータブロック2	75h	0	1	1	0	1 0 1
ECCデータブロック3	55h	0	1	0	1	0 1 0 1
ECCデータブロック4	4Dh	0	1	0	0	1 1 0 1
ECCデータブロック5	55h	0	1	0	1	0 1 0 1
ECCデータブロック8	97h	1	0	0	1	1 1 1 1
修正済セキュリティ情報	55h	0	1	0	1	0 1 0 1

【書類名】 要約書

【要約】

【課題】 セキュリティ性を高めた光ディスク装置のセキュリティ管理方法を提供する。

【解決手段】 読み出し対象となるデータに対するセキュリティ情報を光ディスクの複数箇所から読み出すセキュリティ情報読取工程S22と、複数箇所から読み出されたセキュリティ情報を対比することによって、最も出現頻度の高いセキュリティ情報を正当セキュリティ情報として決定するセキュリティ情報決定工程S24とを含み、正当セキュリティ情報を読み出し対象となるデータの処理に供する光ディクス装置のセキュリティ管理方法によって上記課題を解決できる。

【選択図】 図6

出願人履歴情報

識別番号 [000001889]

1. 変更年月日 1993年10月20日

[変更理由] 住所変更

住 所 大阪府守口市京阪本通2丁目5番5号

氏 名 三洋電機株式会社